Contents

Symmetrische Verschlüsselung

Einführung

Bei der Verschlüsselung unterscheidet man zwischen symmetrisch und asymmetrisch. Bei den Symmetrischen wird im Gegensatz zu den asymmetrischen Verfahren nur ein Schlüssel und somit der gleiche für die Verschlüsselung sowie für die Entschlüsselung verwendet.[1]

Prinzip

Wie schon in der Einführung erwähnt gibt es in der symmetrischen Verschlüsselung nur einen Schlüssel der sowohl für die Ver- als auch für die Entschlüsselung benötigt wird. Somit brauchen Sender und Empfänger den gleichen Schlüssel. Der Sender hat bereits am Anfang des Prozesses den Schlüssel, da er mit diesem ja das Dokument oder die Datei verschlüsselt. Damit der Empfänger den Schlüssel sicher erhält muss ein sicherer Übertragungsweg gewählt werden. Früher wurden diese Schlüssel persönlich, meist mittels eines Boten übermittelt, denn wer den Schlüssel und die Nachricht hat, kann sie auch entschlüsseln.[2]

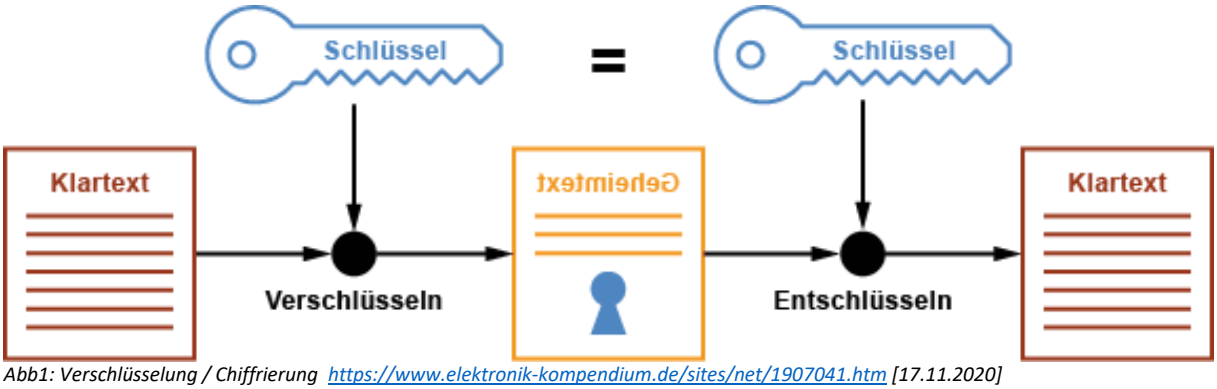

Abb1: Verschlüsselung / Chiffrierung https://www.elektronik-kompendium.de/sites/net/1907041.htm [17.11.2020]

Heutzutage setzt man keine Boten mehr ein, da das persönliche Übergeben sehr umständlich und bei weiten Strecken undenkbar wäre. In der Praxis ist somit eine symmetrische Verschlüsselung nicht mehr denkbar und wird meist mit einem asymmetrischen Verfahren zu einer sogenannten Hybridverschlüsselung kombiniert. Dadurch wird dann der Schlüssel über ein asymmetrisches

[1]Vgl. Symmetrische Verschlüsselung: in: Kryptowissen.de, Absatz 1[online] https://www.kryptowissen.de/symmetrische-verschluesselung.html, [17.11.2020]
[2] Vgl. Symmetrische Verschlüsselung, Prinzip: Absatz 1

Verfahren übergeben um die Nachricht, welche mit dem symmetrischen Verfahren übermittelt wurde, zu entschlüsseln.[3]

Generell unterscheidet man bei der symmetrischen Verschlüsselung zwischen Stromchiffren und Blockchiffren. Bei dem Stromchiffren wird jedes einzelne Zeichen oder jeder einzelne Buchstabe verschlüsselt und bei dem Blockchiffren werden, wie der Name schon sagt, einzelne Blöcke ver- bzw. entschlüsselt.[4]

Vorteile

Der Vorteil der symmetrischen Verschlüsselung ist das einfache Schlüsselmanagement, da es nur ein Schlüssel für die Ent- und Verschlüsselung gibt. Außerdem werden mit diesem Verfahren hohe Geschwindigkeiten bei der Ent- und Verschlüsselung erreicht, weil es meist auf effizienten Operationen wie Bit-Shifts und XORs aufbaut.[5]

Nachteile

Dadurch, dass nur ein Schlüssel verwendet wird, darf dieser nicht in Hände dritter gelangen. Deswegen muss der Schlüssel über einen sicheren Weg übermittelt werden. Die Anzahl der Schlüssel wächst quadratisch, wenn neue Teilnehmer hinzukommen. [6]

Symmetrische Kryptographie

Auch bei der symmetrischen Kryptographie wird ein und derselbe Schlüssel für die Ver- und Entschlüsselung verwendet. In diesem Fall steht man wieder vor dem Schlüsselaustauschproblem. Um die Nachricht zu entschlüsseln braucht man den Schlüssel und hier lauert die Gefahr, dass dieser in Hände Dritter gelangt (durch zum Beispiel abhören der Übertragung). Falls dies passiert kann der Dritte die komplette Nachricht entschlüsseln, abhören oder auch mit einer anderen Verschlüsselung weitersenden. Um dieses Problem zu vermeiden kommt wie schon erwähnt auch hier die hybride Verschlüsselung zum Einsatz.[7]

Angriffe auf das symmetrische Verschlüsselungsverfahren

In Summe gibt es drei verschiedene Angriffsmöglichkeiten um den Schlüssel zu identifizieren: Bei dem Ciphertext-Only Angriff liegt dem Angreifer nur der Geheimtext vor und er versucht durch ausprobieren den Schlüssel zu finden. Die zweite Möglichkeit ist der Known-Plaintext-Angriff. Dort besitzt der Angreifer auch den Geheimtext, aber zusätzlich noch kleinere Teile des Klartextes. In der letzten Möglichkeit besitzt der Angreifer den Geheimtext und zudem noch den kompletten Klartext um den Schlüssel herauszufinden. Dieser Angriff wird Chosen-Plaintext-Angriff genannt.[8]

[3]Vgl. Symmetrische Verschlüsselung, Prinzip: Absatz 2
[4] Vgl. Symmetrische Verschlüsselung, Prinzip: Absatz 3
[5] Vgl. Symmetrische Verschlüsselung, Vorteile: Absatz 1
[6] Vgl. Symmetrische Verschlüsselung, Nachteile: Absatz 1
[7] Vgl. Symmetrische Verschlüsselung: in: Studyflix, Absatz 3 symmetrische Kryptographie [online] https://studyflix.de/informatik/symmetrische-verschlusselung-1610 [17.11.2020c].
[8] Vgl. Symmetrische Verschlüsselung: in: Studyflix, Absatz 9 Angriffe auf symmetrische Verschlüsselungsverfahren [online] https://studyflix.de/informatik/symmetrische-verschlusselung-1610 [17.11.2020c].